NOS. 13-17154, 13-17102

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

FACEBOOK, INC.,

PLAINTIFF-APPELLEE,

V.

POWER VENTURES, INC. AND STEVEN VACHANI,

DEFENDANTS-APPELLANTS.

On Appeal From The United States District Court
for the Northern District of California
Case No. 5:08-cv-05780-LHK
Honorable Lucy H. Koh, District Court Judge

AMICUS CURIAE BRIEF OF ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANTS-APPELLANTS

Cindy A. Cohn, Esq.
cindy@eff.org
Hanni M. Fakhoury, Esq.
hanni@eff.org
ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993

Counsel for Amicus Curiae
Electronic Frontier Foundation

DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER ENTITIES WITH A DIRECT FINANCIAL INTEREST IN LITIGATION

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, amicus curiae Electronic Frontier Foundation states that it does not have a parent corporation, and that no publicly held corporation owns 10% or more of the stock of amicus.

TABLE OF CONTENTS

STATEMENT OF INTEREST 1

INTRODUCTION 2

ARGUMENT 2

I. THERE ARE DISPUTED MATERIAL FACTS ABOUT WHETHER POWER VIOLATED § 502 AND THE CFAA 2

A. Section 502 and the CFAA Must Be Interpreted Narrowly 3

B. Avoiding an IP Address Block Is a Common Technical Measure 4

C. There Should Be No § 502 and CFAA Liability for Circumventing a Technical Barrier That Only Enforces a Terms of Service 10

D. Imposing § 502 and CFAA Liability On a Product That Is Merely Capable of Circumventing A Technical Barrier Puts Innovators at Unnecessary Legal Risk 13

II. POWER DID NOT "INITIATE" "MATERIALLY MISLEADING" MESSAGES UNDER CAN-SPAM. 17

A. This Case Falls Outside the Problem CAN-SPAM Was Addressing. 18

B. Facebook Sufficiently "Initiated" the Messages for Purposes of CAN-SPAM. 21

C. There Are Significant Questions of Fact About Whether the Messages Were "Materially Misleading." 24

D. All Retailers and Individual Users Who Send Commercial Messages Through Facebook are in Violation of CAN-SPAM Under This Theory of Liability. 29

CONCLUSION 31

TABLE OF AUTHORITIES

Federal Cases

Basic, Inc. v. Levinson,
485 U.S. 224 (1988) 25

Brody v. Transitional Hospitals Corp.,
280 F.3d 997 (9th Cir. 2002) 26

Chicago v. Morales,
527 U.S. 41 (1999) 3

Foti v. City of Menlo Park,
146 F.3d 629 (9th Cir. 1998) 10

Gordon v. Virtumundo, Inc.,
575 F. 3d 1040 (9th Cir. 2009) 19, 21, 22

Grayned v. Rockford,
408 U.S. 104 (1972) 4

Griffin v. Oceanic Contractors, Inc.,
458 U.S. 564 (1982) 30

LVRC Holdings LLC v. Brekka,
581 F.3d 1127 (9th Cir. 2009) 11, 14, 15

Mutiven, Inc. v. Cisco Sys., Inc.,
725 F. Supp. 2d 887 (N.D. Cal. 2010) 2

Omega World Travel, Inc. v. Mummagraphics, Inc.,
469 F.3d 348 (4th Cir. 2006) 27, 28

State of California ex rel. Lockyer v. F.E.R.C.,
329 F.3d 700 (9th Cir. 2003) 25

United States v. Gaudin,
515 U.S. 506 (1995) 25

United States v. Ladum,
141 F.3d 1328 (9th Cir. 1998) 25

United States v. Nosal,
676 F.3d 854 (9th Cir. 2012) (en banc) ..... *passim*

United States v. Skilling,
561 U.S. 358 S. Ct. 2896 (2010) 3

United States v. Watkins,
278 F.3d 961 (9th Cir. 2002) 25, 26

Statutes

15 U.S.C. § 7701(a)(1) 19, 24

15 U.S.C. § 7702(8) 22

15 U.S.C. § 7702(9) 22, 23

15 U.S.C. § 7704(a)(1) 21, 22

15 U.S.C. § 7704(a)(1)(B) 22, 24

15 U.S.C. § 7704(a)(2) 22

15 U.S.C. § 7704(a)(3) 22

15 U.S.C. § 7704(a)(5) 22

15 U.S.C. § 7704(a)(6) 26, 28

18 U.S.C. § 1001 25

18 U.S.C. § 1030(a)(2)(C) 14

18 U.S.C. § 1030(a)(4) 15

18 U.S.C. § 1037(a)(1) 18

18 U.S.C. § 1037(a)(3) 18

California Penal Code § 502 ..... *passim*

Legislative Materials

149 Cong. Rec. H12186-02 (Nov. 21, 2003) 20

149 Cong. Rec. S13012-01 (Oct. 22, 2003) 19, 20

149 Cong. Rec. S5175-01 (April 10, 2003) 20

S. Rep. No. 108-102, (2003)
reprinted in 2004 U.S.C.C.A.N. 2348 ..... 19, 20, 23

Other Authorities

American Registry for Internet Numbers, "Internet Number Resource Distribution," May 14, 2012 5

Dan Jerker B. Svantesson, *Geo-Location Technologies and Other Means of Placing Borders on the "Borderless" Internet*, 23 J. Marshall J. Computer & Info. L. 101 (2004) 6

Eric A. Hall, *Internet Core Protocols: The Definitive Guide* (O'Reilly and Associates, 2000) 5

Facebook Statement of Rights and Responsibilities, 9(8), last revised November 15, 2013 13

Jennifer Valentino-Devries, Jeremy Singer-Vine and Ashkan Soltani, "Websites Vary Prices, Deals Based on Users' Information," *Wall Street Journal,* December 24, 2012 7

Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561 (2010) 4

Radia Perlman, *Interconnections, Second Edition* (Addison Wesley Longman, 2000) 5

Simson Garfinkel and Gene Spafford, *Practical Unix and Internet Security*, 484 (O'Reilly and Associates, 1996) 8

Testimony of Seth Schoen before the United States Sentencing Commission (March 17, 2009) 7

Webster's New International Dictionary (3d ed. 1963) 25

STATEMENT OF INTEREST

The Electronic Frontier Foundation ("EFF") is a nonprofit, member-supported civil liberties organization working to protect digital rights. EFF's interest in this case is the principled and fair application of the law to online activities and systems, especially as the law affects both the users of the system and innovators who improve user experience. EFF is especially concerned about Facebook's core claim, accepted by the District Court: that Facebook users who chose to use third parties to automate access to their information stored with Facebook expose the third parties that assist them, and potentially themselves, to serious civil and criminal liability.

Pursuant to Federal Rule of Appellate Procedure 29(c)(5), no one, except for undersigned counsel, has authored the brief in whole or in part, or contributed money towards the preparation of this brief. Neither party opposes the filing of this brief.

INTRODUCTION

Accepting Facebook's claims, the District Court stretched three statutes – California Penal Code § 502, the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030 and the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM"), 15 U.S.C. § 7701, et seq. – far beyond their drafter's intent. Facebook's claims of liability are legally wrong and dangerous as a matter of policy. Because § 502, the CFAA and CAN-SPAM impose significant penalties on violators – including criminal liability – giving these statutes broad application presents a real risk of stifled innovation, legal uncertainty and capricious enforcement. This Court should reverse the grant of summary judgment in favor of Facebook.

ARGUMENT

I. THERE ARE DISPUTED MATERIAL FACTS ABOUT WHETHER POWER VIOLATED § 502 AND THE CFAA.

This Court made clear in *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc) that merely violating a terms of service is inadequate to state a CFAA claim. *Nosal*, 676 F.3d at 863. The same is necessarily true of § 502.[1] The District Court ruled Facebook could prove Power violated § 502 and the CFAA if

[1] The District Court found that the elements of the CFAA are similar to that under § 502. 1-ER 63 (citing *Mutiven, Inc. v. Cisco Sys., Inc.*, 725 F. Supp. 2d 887, 895 (N.D. Cal. 2010)). This brief assumes this is correct.

Power accessed a computer in a manner that overcame a technical or code-based barrier. 1-ER 60, 79.[2]

While some technical restrictions – like requiring a username and password to access information – may state a § 502 and CFAA claim, IP address blocking does not automatically qualify as such. Because there are legitimate reasons for a user to bypass an IP block, the District Court needed to analyze Facebook's reasons for blocking Power more closely. But it failed to make that crucial determination; indeed Facebook never demonstrated that Power's IP address was blocked at all, let alone for a reason other than Power's purported violation of Facebook's terms of service. The District Court's decision instead penalized Power because its code was *designed* to circumvent an IP address block, putting all sorts of innovators at the risk of § 502 and CFAA liability.

A. Section 502 and the CFAA Must Be Interpreted Narrowly.

Both § 502 and the CFAA allow civil and criminal liability. Criminal statutes must be interpreted narrowly to avoid vagueness. *United States v. Skilling*, 561 U.S. 358, 130 S. Ct. 2896, 2927-28 (2010). Vague criminal laws fail to put people on notice on what is prohibited and can encourage "arbitrary and discriminatory enforcement." *Chicago v. Morales*, 527 U.S. 41, 56 (1999) (plurality opinion). Criminal laws must provide "explicit standards for those who

[2] "1-ER" refers to volume 1 of Power's Excerpts of Record.

apply them" because vague laws "impermissibly delegate[] basic policy matters to policemen, judges, and juries for resolution on an ad hoc and subjective basis." *Grayned v. Rockford*, 408 U.S. 104, 108-09 (1972). Vagueness is a particular problem when it comes to the CFAA. *See* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561 (2010).

In *Nosal* this Court feared a broad interpretation of the CFAA "would expand its scope beyond computer hacking to criminalize any unauthorized use of information obtained from a computer." *Nosal*, 676 F.3d at 859. It concluded CFAA liability could not be based on a computer user violating a terms of service or use restriction policy because "significant notice problems arise if we allow criminal liability to turn on the vagaries of private policies that are lengthy, opaque, subject to change and seldom read." *Id.* at 860. It worried "[b]asing criminal liability on violations of private computer use policies can transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved." *Id*.

B. Avoiding an IP Address Block Is a Common Technical Measure.

Since Facebook could not rely on a terms of service violation to prove § 502 or CFAA liability, it instead argued Power circumvented a technical barrier by using multiple IP addresses to access Facebook, including after Facebook attempted to block Power from accessing its site. Apart from being a disputed

factual question, adopting § 502 and CFAA liability for circumventing an IP address runs the risk of criminalizing a perfectly legitimate technical measure.

An "IP address" is a numeric value used to identify a computer or set of computers on the Internet. Internet routers use an IP address to decide where to send communications addressed to a particular computer.[3] The address is normally written as four numbers separated by periods.[4] IP addresses are allocated to Internet service providers (ISPs) in chunks of consecutive addresses out of a worldwide pool of approximately four billion possible addresses.[5] ISPs can further delegate these addresses to smaller entities like a business, Internet café, or smaller ISP.[6] ISPs can also assign an IP address directly to an individual computer. This assignment process is frequently automated and the assignment can be short- or long-term.[7]

Because IP addresses are allocated this way, they convey approximate and general information about a computer's location, how the computer is connected to

---

[3] Eric A. Hall, *Internet Core Protocols: The Definitive Guide*, 37-40 (O'Reilly and Associates, 2000).

[4] Radia Perlman, *Interconnections, Second Edition*, 199 (Addison Wesley Longman, 2000).

[5] American Registry for Internet Numbers, "Internet Number Resource Distribution," May 14, 2012, https://www.arin.net/knowledge/distribution.pdf.

[6] Hall, supra, at 40-41

[7] Wikipedia, "IP Address: IP address assignment," https://en.wikipedia.org/wiki/IP_address#IP_address_assignment.

the Internet or who is using that computer to connect.[8] The IP address used by a particular computer can change over time and individual users connect through different IP addresses depending on where they are. Multiple users can connect to the Internet through a single IP address.[9]

For example, a laptop will receive a different IP address when it connects to the Internet from different locations.[10] If a laptop's owner uses the machine from her workplace in the morning, a café in the afternoon, and her home in the evening, she will use three different IP addresses. A traveler who brings a laptop to a different city and goes online there will receive a different IP address than the one he uses at home. So will an Internet user who changes residential broadband providers, such as switching from Comcast to AT&T. Even a home Internet user may encounter an IP address that changes over time, since some ISPs vary the address they assign to a particular computer on different occasions.[11] Some common Internet technologies such as virtual private networks ("VPN"s) or proxy servers will also change the IP address a user appears to connect from.

---

[8] *See, generally,* Dan Jerker B. Svantesson, *Geo-Location Technologies and Other Means of Placing Borders on the "Borderless" Internet*, 23 J. Marshall J. Computer & Info. L. 101, 109 (2004).

[9] Jeff Tyson, "How Network Address Translation Works," http://computer.howstuffworks.com/nat.htm/printable

[10] University of Illinois Campus Information Technologies and Educational Services, "Network Access While Traveling", http://www.cites.illinois.edu/network/access/travel.html.

[11] Whatismyipaddress.com, "Dynamic IP Addressing," available at http://whatismyipaddress.com/dynamic-static.

There are legitimate reasons for a user to change their apparent IP addresses.[12] The *Wall Street Journal* reported in 2012 that office supplier Staples and hardware store Home Depot used online shoppers' IP address to determine their approximate geographical location and charge consumers different prices depending on that location.[13] Changing an IP address can ensure a consumer is receiving the cheapest price for an item. Similarly, a company may require its employees use a VPN in order to connect to the company's server, ensuring sensitive proprietary documents are secure while travelling over the Internet.

"IP blocking" is the process by which a computer or network ignores all communications from a particular IP address.[14] A server operator could block in order to reduce unwanted Internet traffic based on their belief that particular IP addresses are associated with undesired activity, such as high bandwidth activities like downloading movie files.[15] The operator could refuse communications with a

---

[12] *See* Testimony of Seth Schoen before the United States Sentencing Commission (March 17, 2009), https://www.eff.org/node/56206.

[13] *See* Jennifer Valentino-Devries, Jeremy Singer-Vine and Ashkan Soltani, "Websites Vary Prices, Deals Based on Users' Information," *Wall Street Journal,* December 24, 2012 (Home Depot "said it uses 'IP address,' a number assigned to devices that connect to the Internet, to try to match users to the closest store and align online prices accordingly…Testing suggested that Staples tries to deduce people's ZIP Codes by looking at their computer's IP address.").

[14] *See, generally,* Wikipedia, "Blacklist (computing)," available at http://en.wikipedia.org/w/index.php?title=Blacklist_(computing).

[15] dnsbl.info Spam Database Lookup, available at http://www.dnsbl.info/ (describing publicly-available blacklist databases of IP addresses alleged to have been the origin of large numbers of unwanted spam messages).

particular computer, ISP, or an entire geographic area or country.[16] If a computer has been configured to "block" an IP address, it will either return an error in response to communications from those addresses, stating that a website is unavailable, or ignore those communications entirely and not reply to them.[17] Because it is easy for a user to change her IP address, system administrators know that IP blocking is an easily ignored tool for limiting Internet connections.[18] Requiring a username and password, as Facebook does, is a better way of distinguishing between authorized and unauthorized users.

Internet users who find their computers blocked from accessing a particular service may have many reasons to try to circumvent the block by doing something as simple as logging in from a different place. An employer might have a policy that a certain service may be accessed only from specific locations and could block all unknown IP addresses to implement the policy. An employee traveling to a new location could use a proxy or VPN service to change the apparent IP address in order to access the service.

---

[16] *See, generally,* Wikipedia, "IP blocking," available at https://en.wikipedia.org/wiki/IP_address_blocking.

[17] "Yahoo! Help Article, IP Address Blocking," available at http://help.yahoo.com/l/us/yahoo/smallbusiness/store/risk/risk-17.html .

[18] Simson Garfinkel and Gene Spafford, *Practical Unix and Internet Security*, 484 (O'Reilly and Associates, 1996) ("Restricting a service by IP address or hostname is a fundamentally unsecure way to control access to a server.").

An American bank's anti-fraud measures could categorically forbid access to online banking services from certain foreign countries which have high rates of fraud by blocking all IP addresses associated with those countries. A legitimate customer of the bank, frustrated at the inability to log on to the bank's website during a trip, could use a proxy or VPN to bypass the restriction by appearing to connect from a U.S.-based IP address.

A user often has no way of knowing why a block is in place, or whether that block is aimed at them specifically. In the case of the bank above, the IP block is likely not aimed at a legitimate bank customer. Yet this user has no way of knowing why he is being denied access, or whether that denial was due to a technical problem or an intentional block.

These examples illustrate there is nothing inherently improper or unlawful about switching IP addresses to avoid an IP block and there can be notice problems with determining the reason for the block. The means of switching – going to a different location, using a VPN or proxy server, asking the ISP to allocate a different address – are common and do not interfere with the proper functioning of the blocking server.

C. There Should Be No § 502 and CFAA Liability for Circumventing a Technical Barrier That Only Enforces a Terms of Service.

The question, then, is whether evading IP blocking to allow authorized users access to their own data through "automatic means," without causing any harm, violates § 502 or the CFAA. The answer must be no.

Power did nothing more than provide Facebook users with a way to control and access their own data. Power only accessed data at the request of Facebook users who knowingly and deliberately used Power's service. A Facebook user had to provide his own valid username and password through Power in order to obtain access to his Facebook data. The IP blocking here was done for no reason other than Facebook did not approve of the way Power allowed Facebook users to access its own data. There was no allegation that Power was accessing data without a user's knowledge and permission.

In finding Power liable under § 502 and the CFAA, the District Court created another variation of the problem in *Nosal*: companies can now "transform whole categories of otherwise innocuous behavior into federal crimes" through code instead of words. *Nosal*, 676 F.3d at 860. As a result, the public is unable to distinguish in a meaningful and principled way between innocent and criminal activity. *See Foti v. City of Menlo Park*, 146 F.3d 629, 638 (9th Cir. 1998). Just as violating a terms of service does not create § 502 or CFAA liability, neither does

bypassing an IP block where Facebook users have authorized Power to access Facebook data on their behalf.

This is not to say that § 502 or the CFAA could *never* prohibit bypassing a technological block. If a service provider blocked to prevent access by unauthorized persons who evaded that block in order to gain access, that person may have violated § 502 or the CFAA. If a third party helped that unauthorized user evade a technical block, it too could be liable.

Unfortunately, the District Court did not look to Facebook's purpose in blocking Power's IP address. Nor did it consider that the Facebook users being blocked were entitled to access their own Facebook data. It did not determine whether Power was ever put on notice for the reason why it had been blocked before determining Power was liable under § 502 and the CFAA. Instead it found Facebook's motivation in implementing a technological barrier irrelevant. 1-ER 83. It believed there could "be no ambiguity or mistake as to whether access has been authorized when one encounters a technical block." *Id.* This was error.

This Court in *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009) made clear the computer owner bears the responsibility of actually creating a barrier that puts a user on notice that their access is "unauthorized" under the CFAA. *Brekka*, 581 F.3d at 1135 ("The plain language of the statute . . . indicates that 'authorization' depends on actions taken by the [computer owner].").

Considered with *Nosal's* specific concern about computer users not having notice as to what acts violate the CFAA, courts must dig deeper, looking to the purpose and language of § 502 and the CFAA, and the effect of a technological barrier, before determining whether evading that barrier violates these statutes. If a particular technological restriction seeks to control access to or use of data from an entity unauthorized to obtain it, and the person has notice of that fact, then evasion of the technological restriction is likely criminal. That would include, for instance, an unauthorized person attempting to bypass a username and password prompt by trying different combinations until it can access data it is otherwise not entitled to have.

However, if the technical restriction merely seeks to impose owner preferences or terms of service on otherwise authorized users, like the IP blocking here, than there is no § 502 or CFAA liability. Holding otherwise gives website owners the power to criminalize any term of service that could be implemented in code regardless of whether the user was authorized or the term imposed a restriction that criminal law should not be used to enforce.

Enforcing private website operators' preferences with criminal law puts immense coercive power behind terms and conditions, and technological measures that may be contrary to the interests of consumers and the public. Many terms of service contain conditions that are vague and arbitrary. *See Nosal*, 676 F.3d

at 862. Facebook itself tells developers using Facebook data that it "can require you to delete user data if you use it in a way that we determine is inconsistent with users' expectations."[19] Terms of service are not written with the precision and care required of a criminal statute. Nor are such terms necessarily written with the public interest in mind. Technological measures like IP blocking are even more imprecise since they give the user no understanding of why they have been implemented.

Thus, the mere circumvention of an IP block, without more analysis, is not enough to state a claim under § 502 or the CFAA.

D. Imposing § 502 and CFAA Liability On a Product That Is Merely Capable of Circumventing A Technical Barrier Puts Innovators at Unnecessary Legal Risk.

Even if this Court rules circumventing a technical barrier that merely enforces a term of service is enough to state § 502 and CFAA liability, the District Court erred in finding liability when there was clearly contested issues of material fact about whether Power *actually* circumvented a technical block in the first place. Facebook claimed once it blocked Power's primary IP address, it determined Power was circumventing the block by using other IP addresses. 1-ER 61. Power claimed its use of other IP addresses to access Facebook was not designed to circumvent a Facebook block but rather was part of Power's normal course of

[19] Facebook Statement of Rights and Responsibilities, 9(8), last revised November 15, 2013, https://www.facebook.com/legal/terms.

business. According to Power, once it determined that Facebook was attempting to prevent it from accessing Facebook's site, it undertook steps to follow Facebook's requests to obtain access to Facebook data. *Id.* at 61-62.

Despite this disputed evidence, the District Court ruled there was "overwhelming evidence" that Power "designed their system to render [IP] blocks ineffective." *Id.* at 62. It found there was "no reason to distinguish between methods of circumvention built into a software system to render barriers ineffective and those which respond to barriers after they have been imposed." *Id.* Coupled with statements that Power anticipated Facebook would attempt to block Power, merely implementing a system that could bypass Facebook's blocks was enough for § 502 and CFAA liability. *Id.*

Writing code that is capable of circumventing a technical barrier, but never actually does so or even *attempts* to do so, cannot make access "without permission" or "unauthorized." Under *Brekka* and *Nosal*, "authorization" does not turn on the mental state of the party accessing the computer, or the purpose for which they access data.[20] That is especially true here because the District Court found Power liable under 18 U.S.C. § 1030(a)(2)(C), which only prohibits

[20] The mindset of the party accessing data is relevant in determining whether they "intentionally" accessed a protected computer under 18 U.S.C. § 1030(a)(2)(C) or "knowingly access[ed]" a computer under § 502(c). But that is a separate issue from the question of "permission" or "authorization" and there is no dispute that Power acted "intentionally" and "knowingly."

accessing data "without authorization" from a computer. It specifically declined to rule whether Power violated 18 U.S.C. § 1030(a)(4), which requires intent to defraud. 1-ER 13, 63-64.

By focusing on Power's design rather than what it actually did in response to Facebook's purported IP blocking, the District Court effectively ignored *Brekka* and *Nosal*, instead making it a "thought crime" to produce a tool capable of circumventing any technical barrier a service might create in the future. Thus, although Power was technically able to access data as the agent of a Facebook user, and before Facebook took any steps to affirmatively block Power from accessing Facebook data – a clearly contested material fact – the District Court nonetheless found Power was not "authorized" to access data because it designed its code to circumvent hypothetical technical blocks.

This broad theory of liability chills follow-on innovators who seek to create tools to improve a user's experience with a particular service. Any follow-on innovation that could potentially bypass a technological restriction, regardless of whether that design choice was innocent or ill-intentioned, could face § 502 and CFAA liability. Innovators would be forced to anticipate every technical block that any interoperable system or program could impose and avoid building any tool that could possibly bypass those measures. This unworkable, unconstitutional rule would render these computer crime laws void for vagueness.

Moreover, this Court should be careful not to suggest criminal liability attaches when a user or user-directed service violates a term or condition that seeks to, or effectively does, prohibit competing or follow-on innovation. Facebook's theory of § 502 and CFAA liability prevents users from adopting follow-on innovation by third parties, running the very serious risk of excluding competition and limiting users to only Facebook approved innovation.

More worrisome, by stopping users from engaging the assistance of third parties and automated systems like Power's to access and remove their data, Facebook increases the cost to consumers of switching social networking services. Imposing criminal liability on users who select tools that enable them to easily access or move their Facebook data poses unacceptable risks to consumers and innovators. Consumer choice would be limited not by natural competition, but a social network's privately imposed – but publicly enforced – terms, for which the penalty for non-compliance is unacceptably steep. Companies garner and keep customer loyalty by providing a quality product. If the product is substandard or something better comes along, customers can vote with their feet and shop elsewhere. The ability to choose what services to use and how to use them is good for customers and healthy for businesses.

The District Court's interpretation of § 502 and the CFAA interferes with market forces that would otherwise allow users to freely leave the service if, for

example, they dislike changes in Facebook's terms of use or privacy policies.[21] Its finding of § 502 and CFAA liability must be reversed.

II. POWER DID NOT "INITIATE" "MATERIALLY MISLEADING" MESSAGES UNDER CAN-SPAM.

Facebook runs a "captured" email program. The emails sent by users through Facebook's system, whether for commercial or noncommercial purposes, will *always* indicate they came from Facebook, rather than from the original sender. Facebook controls the From and Subject lines, requires the text to be signed "The Facebook Team," and includes links to its own system—not the user's or in this case Power's system—for opt-out purposes. This is a function of Facebook's design decisions, which is not under the control of the sender or recipient. In this way, Facebook, while allowing email to be sent, is not like a traditional Internet service provider's email system. CAN-SPAM was passed in 2004 the same year that Facebook launched and long before it reached the widespread popularity it enjoys today. Thus the problem before this Court: applying Congressional language based on assumptions about how an ISP works to a new technological configuration that does not follow those assumptions.

[21] These concerns are not merely hypothetical. Facebook has consistently sparked protest when it changes its terms of use and practices that made users' personal data increasingly accessible to third parties, including advertisers. While Facebook may have the right to make these changes, its users certainly have the right to leave, and take their data with them if they disapprove.

The District Court found Power violated CAN-SPAM because it "initiated" email messages that contained "misleading" header information – the messages claimed to be sent from Facebook with an @facebookmail.com return address, when in reality the messages were sent by Facebook users through Power. But the district court was wrong both that Power "initiated" the messages and that the messages, in context, were "materially misleading" for purposes of CAN-SPAM. The implications of finding Power liable for acts in Facebook's control are severe, not just for Power but for the hundreds of millions of other users of Facebook, or any other captured email system.

As with § 502 and the CFAA, because CAN-SPAM creates both civil and criminal liability, this Court has to interpret it narrowly, especially when it would "criminalize a broad range of day-to-day activity." *Nosal*, 676 F.3d at 863.[22] That means this Court should find Power did not violate CAN-SPAM.

A. This Case Falls Outside the Problem CAN-SPAM Was Addressing.

When CAN-SPAM was introduced, Congress clearly believed there were "beneficial aspects to commercial e-mail, even bulk messaging that Congress

[22] *See* 18 U.S.C. § 1037(a)(1) (crime to "access[] a protected computer without authorization, and intentionally initiate[] the transmission of multiple commercial electronic mail messages from or through such computer"); 18 U.S.C. § 1037(a)(3) (crime to "materially falsif[y] header information in multiple commercial electronic mail messages and intentionally initiate[] the transmission of such messages").

wanted to preserve, if not promote." *Gordon v. Virtumundo, Inc.*, 575 F. 3d 1040, 1049 (9th Cir. 2009). CAN-SPAM itself acknowledges email is an

> extremely important and popular means of communication, relied on by millions of Americans on a daily basis for personal and commercial purposes. Its low cost and global reach make it extremely convenient and efficient, and offer unique opportunities for the development and growth of frictionless commerce.

15 U.S.C. § 7701(a)(1); *see also* S. Rep. No. 108-102, at 2 (2003), *reprinted in* 2004 U.S.C.C.A.N. 2348, 2349 ("Unlike direct mail delivered through the post office to consumers, [e-mail] can reach millions of individuals at little to no cost and almost instantaneously.").

Congress also recognized that unsolicited "spam" emails were a growing problem, "a favored mechanism of those who seek to defraud consumers and make a living by preying on unsuspecting e-mail users and those new to the Internet," as well as bombard unsuspecting users with "objectionable" content like pornography. 2004 U.S.C.C.A.N. at 2349. These types of messages presented a risk of "exposure and sharing of sensitive personal information over the Internet, and credit card or identity theft." *Id.* at 2352. Congress worried that spam could be "used to lure unwary users to websites that contain viruses, spyware, or other malicious computer code." *Id.* It identified the problem as a "few hundred" big spammers or "kingpins" sending deceptive and misleading spam messages. *See, e.g.,* 149 Cong. Rec. S13012-01 (Oct. 22, 2003) (statement of Sen. Wyden)

(referring to "kingpin" and "big-time spammers" as source of the problem); *id.* (statement of Sen. Schumer) ("the good news is that since we know that a large amount of spam comes from a small amount of people, we can get after these few people").

Congress was especially concerned consumers would not know where spam was coming from or how to make it stop. The Senate Report noted

> the inconvenience and intrusiveness to consumers of large volumes of spam are exacerbated by the fact that, in many instances, the senders of spam purposefully disguise the source or content of the e-mail by falsifying or including misleading information in the e-mail's [header] lines. Thus, the recipient is left with no effective ability to manage the inflow of spam…because he or she cannot often tell without opening the individual messages who is sending the messages or what they contain.

2004 U.S.C.C.A.N. at 2350. It cautioned "most consumers do not have any way to dependably contact the senders to instruct them to take the recipient off their mailing lists." *Id.* Congress also worried about spammers disguising their identity to mask the true source of the messages. *See* 149 Cong. Rec. H12186-02 (Nov. 21, 2003) (statement of Mr. Dingell) (CAN-SPAM "prohibits false and misleading transmission information so that marketers cannot hide their identity"); 149 Cong. Rec. S5175-01 (statement of Mr. Wyden) (April 10, 2003) (CAN-SPAM "would prohibit the use of falsified or deceptive headers or subject lines, so that consumers will be able to identify the true source of the message.").

This legislative history shows what CAN-SPAM was truly aimed at: deceptive and fraudulent email practices foisted upon unsuspecting users. The stringent criminal and civil penalties in CAN-SPAM demonstrate the extent to which Congress was aimed at clearly bad actors and intentional efforts taken to hide the origin of messages.

But that is not what happened here. These messages were not deceptive. Facebook users utilizing Power's service made a conscious choice to send Event invitations to other Facebook users and the messages themselves were clear that they were promoting Power's service. This sort of viral marketing is not what CAN-SPAM was intended to punish.

B. Facebook Sufficiently "Initiated" the Messages for Purposes of CAN-SPAM.

Ultimately, CAN-SPAM did not "ban spam outright, but rather provides a code of conduct to regulate commercial e-mail messaging practices." *Gordon*, 575 F.3d at 1048. Relevant here, it is unlawful for a person "to initiate the transmission, to a protected computer, of a commercial electronic mail message" that contains "header information that is materially false or materially misleading." 15 U.S.C. § 7704(a)(1). "Header information" means "the source, destination, and routing information attached to an electronic mail message, including the originating domain name and originating electronic mail address, and any other information that appears in the line identifying, or purporting to identify, a person

initiating the message." 15 U.S.C. § 7702(8). But as long as the "from" line "accurately identifies any person who initiated the message," the message will not be "materially false or misleading" under CAN-SPAM. 15 U.S.C. § 7704(a)(1)(B).

Implicit in CAN-SPAM's obligations is that the person who "initiates" the message will have control over the header, the subject heading and the inclusion of identifiers, opt-outs and return addresses. "Initiate" means "to originate or transmit such message or to procure the origination or transmission of such message." 15 U.S.C. § 7702(9). The person who "initiates" a commercial email cannot use materially misleading header information, 15 U.S.C. § 7704(a)(1), use a deceptive subject heading, 15 U.S.C. § 7704(a)(2), omit a return email address, 15 U.S.C. § 7704(a)(3), or fail to include a clear identification that the message is an advertisement, provide an opportunity to opt-out of the mailing and list a physical address of the sender. 15 U.S.C. § 7704(a)(5); *see generally Gordon*, 575 F.3d at 1048. If the message sender could not control these features, CAN-SPAM liability would not deter anyone with the threat of statutory damages or criminal liability.

The District Court found Power "initiated" a commercial email with "materially false or materially misleading" header information when it sent the Event invitations as part of its marketing campaign to get users to sign up to Power's service. 1-ER 55-59. Although the messages were authorized by

Facebook's users and sent from Facebook's own server, it found Power had nonetheless "initiated" the messages because it intentionally caused Facebook's servers to send the messages and encouraged used to send the messages by offering a $100 reward to those who got a certain number of friends signed up. *Id.* at 56-57.

More than one person can "initiate" a message for purposes of CAN-SPAM. *See* 15 U.S.C. § 7702(9). The Senate Report provides an example: "if one company hires another to handle the tasks of composing, addressing, and coordinating the sending of a marketing appeal, both companies could be considered to have initiated the message–one for procuring the origination of the message; the other for actually originating it." 2004 U.S.C.C.A.N. at 2360. But a company "that merely engages in routine conveyance, such as an ISP that simply plays a technical role in transmitting or routing a message and is not involved in coordinating the recipient addresses for the marketing appeal, shall not be considered to have initiated the message." *Id.*

Facebook plays more than a mere technical role here and is properly considered an "initiator" of the messages. Due entirely to Facebook's own design of its Event and messaging systems, the portions of the messages that allegedly violate CAN-SPAM are set by Facebook and not controlled by Power at all. As noted above, Facebook controls the From and Subject lines, requires the text to be

signed "The Facebook Team," and includes links to its own system—not the user—for opt-out purposes. Ultimately, that means Facebook has sufficiently "initiated" the messages for purposes of CAN-SPAM.

Because the messages "accurately identifies any person who initiated the message" – specifically Facebook – they cannot be "materially false or materially misleading" under CAN-SPAM. *See* 15 U.S.C. § 7704(a)(1)(B).

C. There Are Significant Questions of Fact About Whether the Messages Were "Materially Misleading."

Even if this Court disagrees that Facebook "initiated" the messages, they were not "materially misleading". The District Court found the messages were "misleading" as to who initiated them because although Power "initiated" the message, they came from an @facebookmail.com address and did not contain any return address that would allow a recipient to respond to Power directly. 1-ER 57-58. Notably it nowhere addressed whether the messages were "*materially* misleading," the relevant CAN-SPAM standard. 15 U.S.C. § 7704(a)(1) (emphasis added). Although the text of the messages had information about Power, the District Court believed this was irrelevant since the presence of a misleading header is itself enough to prove a CAN-SPAM violation. 1-ER 58. But the District Court was wrong; the reference to Power in the text of the messages was relevant to determining whether the messages were "materially misleading."

CAN-SPAM does not define the words "material" or "misleading" but the phrases are common ones in federal law. When Congress "borrows terms of art in which are accumulated the legal tradition and meaning of centuries of practice" it knowingly adopts "the cluster of ideas that were attached to each borrowed word." *State of California ex rel. Lockyer v. F.E.R.C.*, 329 F.3d 700, 709, n. 7 (9th Cir. 2003).

For purposes of the crime of making a false statement under 18 U.S.C. § 1001, a statement is "material" if it has a "a natural tendency to influence, or [be] capable of influencing, the decision of the decisionmaking body to which it was addressed." *United States v. Gaudin*, 515 U.S. 506, 509 (1995). The statement must "under some set of foreseeable circumstances, *significantly affect* an action." *United States v. Ladum*, 141 F.3d 1328, 1335 (9th Cir. 1998) (quotations omitted) (emphasis added). Similarly, for securities fraud, "materiality" requires a "substantial likelihood that the disclosure of the omitted fact" would have "*significantly altered* the 'total mix' of information made available." *Basic, Inc. v. Levinson*, 485 U.S. 224, 231-32 (1988) (quotations omitted) (emphasis added).

To be "misleading," a statement must "lead in a wrong direction or into a mistaken belief." *United States v. Watkins*, 278 F.3d 961, 967 (9th Cir. 2002) (quoting Webster's New International Dictionary 1444 (3d ed. 1963) (quotations

omitted)). To "mislead" generally requires "materiality" as well because one "cannot 'intend to mislead' another by means of a misrepresentation without having an expectation that the recipient would actually or reasonably rely on it." *Watkins*, 278 F.3d at 966; *see also Brody v. Transitional Hospitals Corp.*, 280 F.3d 997, 1006 (9th Cir. 2002) ("misleading" for purposes of securities law requires "an impression of a state of affairs that differs in a *material* way from the one that actually exists.") (emphasis added).

In short, trivial misrepresentations that do not create a false impression with the person that something is one way when it really is another is necessary for a header to be "materially misleading" for purposes of CAN-SPAM. While CAN-SPAM does not define "materiality," it does note misleading header information includes information that impairs the ability "to identify, locate, or respond to a person who initiated the electronic mail message or to investigate the alleged violation, or the ability of a recipient of the message to respond to a person who initiated the electronic message." 15 U.S.C. § 7704(a)(6). That is consistent with the aim of CAN-SPAM: ensuring consumers could determine who is sending deceptive and offensive emails.

Judged under these stringent standards, the messages sent by Power are not "materially misleading." The messages had clear sources: the user who sent the message and Facebook who acted as the intermediary. In the one area of the Event

invitation Power could control, it clearly identified itself as the "host of the event and the event location." 1-ER 56. A recipient has a clear path to make the messages stop by following the links at the bottom of the messages to opt out through Facebook's internal system. Or the recipient of an unwanted invitation could ask their friend not to send further invitations. In other words, far from being a spammer "purposefully disguising" itself from detection, Power took every practical step available under Facebook's system to identify itself. Unsurprisingly, there was no evidence that any Facebook user felt mislead by these specific invitations. 1-ER 31, 53.

The Fourth Circuit in *Omega World Travel, Inc. v. Mummagraphics, Inc.*, 469 F.3d 348 (4th Cir. 2006) considered and rejected a similar claim to the one brought by Facebook here. An ISP brought suit against a travel agency for inaccuracies in commercial emails sent by Cruise.com, a website that sold cruise vacations. 469 F.3d at 350-51. The ISP claimed the message headers were "materially false or materially misleading" because they incorrectly identified the originating email server and the messages appeared to come from a nonfunctional email address. *Id.* at 357.

The Fourth Circuit agreed with the district court that these inaccuracies did not create CAN-SPAM liability because the messages "were chock full of methods to 'identify, locate, or respond to' the sender or to 'investigate [an] alleged

violation' of [CAN-SPAM]." *Id.* (quoting 15 U.S.C. 7704(a)(6)). The messages referenced Cruise.com and its website, which was no surprise because the whole point of the advertisements was "to induce recipients to contact Cruise.com to book the cruises that the messages advertised." *Id.* at 358. The court believed that finding "the alleged inaccuracies in a message containing so many valid identifiers could be described as 'materially false or materially misleading,'" under CAN-SPAM would make the materiality requirement "meaningless." *Id.*

Similarly here, the messages were not "materially misleading." The messages clearly identified all three entities involved with the message: the individual user inviting their friend, Facebook as an intermediary and Power as the "host" of the Event. Like Cruise.com, in order for Power's promotion to work and gain attention and new users, Power would necessarily need to highlight its services. Unlike the true spammers CAN-SPAM was intended to go after – "kingpins" hiding their identity in order to defraud and cheat email recipients – Power wanted Facebook users to know its product existed. Most importantly, there was no evidence that anyone complained to Facebook about the specific messages.

Contrary to the District Court's belief, the fact the messages contained information clearly identifying Power was relevant for determining whether Power violated CAN-SPAM.

D. All Retailers and Individual Users Who Send Commercial Messages Through Facebook are in Violation of CAN-SPAM Under This Theory of Liability.

Given the way Facebook implemented its messaging system, a company that uses Facebook's Event system to send a commercial invitation will always be "initiating" a message with a "misleading" header for purposes of CAN-SPAM because although the message will be sent by someone else, it will return an @facebookmail.com address and contain links to Facebook's system, not the company's. Given Facebook's success at recruiting companies to advertise on its site and reach out to the company's enormous user base, Facebook's selective use of CAN-SPAM to pursue Power appears to be motivated by, at best, annoyance with Power, and at worst, purely anti-competitive purposes. But there is no limit on Facebook's ability to use the threat of CAN-SPAM liability on users it disfavors for any reason it chooses.

More problematic is the fact the District Court's decision means that individual users who compose Event invitation are in violation of CAN-SPAM. After all, it was the individual user who truly "initiated" the Event invitation by clicking on a link, choosing which of his friends should be sent an invitation, and then clicking "send." The District Court even suggested the users were "initiators" of the messages too. 1-ER 56-57. The end result is that ordinary and everyday uses of Facebook and other forms of social media can easily run afoul of CAN-

SPAM by simply "inviting" one's friends to enjoy third party commercial products, services or promotions.

For example, say a local band wants to use Facebook's Events feature to publicize a show with a small cover charge, and band members invite their Facebook friends. Given the way Facebook's Event system works, the Event invitation will look like it came from Facebook, contain an @facebookmail.com return address and opt-out links corresponding to Facebook. The District Court's CAN-SPAM theory means this user "initiated" a message with a misleading header despite the fact she cannot control the header. That user is now liable under CAN-SPAM for $100 in statutory damages for each friend she invites to the show. It is not just Facebook; the District Court's decision enables any developer of a captive messaging system to design its messaging system to ensure messages do not comply with CAN-SPAM and then threaten to sue commercial users it disfavors or competes against.

Courts must avoid "interpretations of a statute which would produce absurd results." *Griffin v. Oceanic Contractors, Inc.*, 458 U.S. 564, 575 (1982). *Nosal* already warned about interpreting computer crime laws in ways that "criminalize a broad range of day-to-day activity." *Nosal*, 676 F.3d at 863. The theory of CAN-SPAM liability here should be rejected and this Court should reverse the summary judgment finding in favor of Facebook.

CONCLUSION

For the reasons stated above, this Court should reverse the District Court's grant of summary judgment to Facebook.

Dated: March 10, 2014

By: */s/ Hanni M. Fakhoury*
Hanni M. Fakhoury
Cindy A. Cohn
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993
hanni@eff.org

Attorneys for Amicus Curiae Electronic Frontier Foundation

**CERTIFICATE OF COMPLIANCE
WITH TYPE-VOLUME LIMITATION,
TYPEFACE REQUIREMENTS AND TYPE STYLE REQUIREMENTS
PURSUANT TO FED. R. APP. P. 32(a)(7)(C)**

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify as follows:

1. This Brief of Amicus Curiae In Support Of Defendant-Appellant complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 6,984 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2011, the word processing system used to prepare the brief, in 14 point font in Times New Roman font.

Dated: March 10, 2014

By: */s/ Hanni M. Fakhoury*__

Hanni M. Fakhoury
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993
hanni@eff.org

Attorneys for Amicus Curiae Electronic Frontier Foundation

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on March 10, 2014.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: March 10, 2014

By: */s/ Hanni M. Fakhoury*__

Hanni M. Fakhoury
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94110
Telephone: (415) 436-9333
Facsimile: (415) 436-9993
hanni@eff.org

Attorneys for Amicus Curiae Electronic Frontier Foundation